Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	24. september 2026

Sak 112-2026

Det digitale trusselbildet mot spesialisthelsetjenesten 2026

Forslag til vedtak:

Styret tar rapporten *Trusselvurdering for spesialisthelsetjenesten 2026* til etterretning, og ber om at den legges til grunn for sikkerhets- og risikostyringen i foretaksgruppen.

Hamar, 17. september 2026

Terje Rootwelt
administrerende direktør

1 Hva saken gjelder

Sykehuspartner HF er i oppdrag og bestilling bedt om å benytte spesialisthelsetjenestens trusselvurdering i arbeidet med digital sikkerhet.

Trusselvurderingen gir viktig innsikt som skal benyttes i arbeidet med sikkerhets- og risikostyring i regionen, sikring av infrastruktur og tjenester og for å etablere grunnleggende sikkerhetsbarrierer som beskytter mot digitale angrep.

Trusselvurdering for spesialisthelsetjenesten 2026 beskriver de mest relevante truslene som kan påvirke spesialisthelsetjenestens evne til å yte gode, trygge og effektive helsetjenester.

Arbeidet med trusselvurderingen, herunder innhenting og analyse, har foregått fra september 2025 til 14. april 2026.

2 Hovedpunkter og vurdering av handlingsalternativer

Etterretning- og sikkerhetstjenestene (EOS-tjenestene) understreker at sikkerhetssituasjonen i Norge er mer krevende enn på lenge. Dette er noe vi også ser i spesialisthelsetjenesten, både med hensyn til trusler som treffer oss, og uroligheter knyttet til den sikkerhetspolitiske situasjonen.

Årets trusselvurdering for spesialisthelsetjenesten har derfor en annen oppbygging enn tidligere og inkluderer mer enn cyberbaserte trusler. Dette gir oss en bedre forståelse av hvilke trusler spesialisthelsetjenesten står ovenfor, og hvordan trusselaktørene kan endre motivasjon og målutvelgelse.

Komplekse utfordringer i en usikker tid
I likhet med i fjor, inneholder trusselvurdering et kapittel med vurderinger knyttet til geopolitisk ustabilitet.

Fortsatt usikkerhet i det sikkerhetspolitiske samarbeidet
Stormakter prioriterer i økende grad egne interesser og bruker makt til å nå sine mål. Det er hardere konkurranse om makt og innflytelse mellom demokratiske og autoritære krefter, trusselbildet er mer komplekst, og vi ser mer uregulert maktbruk. I takt med at amerikansk politikk blir stadig mer uforutsigbar kommer trusselen mot vestlige demokratier ikke lenger bare fra Kina og Russland.

Sammensatte trusler og sammensatt virkemiddelbruk
Sammensatte trusler er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt. Vi ser at trusselaktørenes vilje og evne til å bruke sammensatte virkemidler har økt i perioden fra siste rapport.

Helseberedskap og totalforsvaret
Norge har én, samlet offentlig helsetjeneste som skal virke i hele krisespekteret og yte helsetjenester for både sivilbefolkningen og Forsvaret. Behovet for digital motstandskraft øker som følge av den sikkerhetspolitiske situasjonen og omfanget av digitale sårbarheter og cyberangrep. Spesialisthelsetjenesten er en del av grunnberedskapen i Norge og en sentral aktør i arbeidet med å håndtere kriser.

Konsentrasjonsrisiko
Virksomheter som understøtter grunnleggende nasjonale funksjoner, kan ha betydelige avhengigheter, gjennom verdikjeder og strategiske knutepunkter, til land som utgjør en etterretningstrussel mot Norge. Avhengigheter til enkeltleverandører og enkeltland kan medføre økt risiko for bortfall av tjenester, noe som kan brukes for å utøve press og påvirkning. Trusselaktører kan utnytte bortfall i leveranser til virksomheter som et pressmiddel.

Metode
Trusselaktørene benytter et bredt spekter av metoder for å få tilgang til virksomheters systemer, data og digitale tjenester. Metodene spenner fra teknisk kompromittering av systemer og infrastruktur til sosial manipulering av brukere og utnyttelse av kunstig intelligens for å effektivisere og skalere angrep. I spesialisthelsetjenesten rammer dette et sammensatt digitalt miljø der kliniske systemer, medisinsk-teknisk utstyr, skytjenester, mobile arbeidsflater og eksterne leverandører er tett integrert. Dette gir store gevinster for pasientbehandling og drift, men skaper samtidig en stor og kompleks angrepsflate.

Flere av angrepsmetodene forsterker hverandre. Sosial manipulering kan gi innledende tilgang som senere brukes til teknisk kompromittering, mens kompromitterte kontoer, sårbare systemer eller leverandørforhold kan gi videre tilgang til større deler av virksomhetens digitale miljø. Samtidig gjør økt bruk av kunstig intelligens det mulig for trusselaktører å arbeide raskere, mer målrettet og i større skala enn tidligere. For spesialisthelsetjenesten innebærer dette at trusselbildet blir mer sammensatt, mer dynamisk og mer krevende å oppdage og håndtere. Det stiller økte krav til forebygging, innsyn, motstandsevne og evne til rask respons på tvers av systemer, brukere og verdikjeder.

2.1. Hovedvurderingene i rapporten

- **Trusselen mot spesialisthelsetjenesten fra organisert cyberkriminalitet er meget høy**
  Spesialisthelsetjenesten er et ettertraktet og utsatt mål, og vi forventer økt oppmerksomhet fra utpressingsgrupper og deres samarbeidspartnere i kommende periode. Vi vurderer det som **meget sannsynlig** at spesialisthelsetjenesten vil bli utsatt for angrepsforsøk fra organisert kriminalitet og at trusselen er **meget høy**.

- **Trusselen mot spesialisthelsetjenesten fra cyberspionasje er høy**
  Statlige aktører gjennomfører cyberspionasjekampanjer mot vestlig helsevesen, noe vi tidligere har observert mot spesialisthelsetjenesten i Norge. Vi forventer at spesialisthelsetjenesten i Norge vil være et mål i 2026. Trusselen fra cyberspionasje mot spesialisthelsetjenesten er **høy**, og det er **meget sannsynlig** at spesialisthelsetjenesten vil utsettes for cyberspionasje fra aktører med direkte eller indirekte koblinger til russiske og kinesiske etterretningsorganisasjoner.

- **Trusselen mot spesialisthelsetjenesten fra innsidevirksomhet er høy**
  Spesialisthelsetjenesten er en sentral aktør i totalforsvaret og råder i tillegg over verdier med betydning for nasjonal sikkerhet. Vi vurderer at dette samlet sett gjør spesialisthelsetjenesten til et attraktivt mål for trusselaktører, som vil kunne ha stor nytte av å plassere innsidere i spesialisthelsetjenesten. Innhenting av informasjon gjennom rekruttering av innsidere utgjør en **høy** trussel mot spesialisthelsetjenesten. Dette gjør at vi vurderer det som **sannsynlig** at spesialisthelsetjenesten vil bli utsatt for innsidevirksomhet.

- **Trusselen mot spesialisthelsetjenesten fra destruktive cyberangrep og sabotasje er moderat**
  Den sikkerhetspolitiske situasjonen i verden bidrar til at statlige aktører har økt vilje til å bruke sammensatte virkemidler. Trusselen fra destruktive cyberangrep og sabotasje mot spesialisthelsetjenesten er **moderat,** og det er **mulig** at slike angrep vil kunne ramme spesialisthelsetjenesten direkte eller indirekte i 2026.

- **Trusselen mot spesialisthelsetjenesten fra hacktivisme er moderat**
  Det har ikke vært hacktivistangrep rettet direkte mot spesialisthelsetjenesten i foregående periode. Vi har imidlertid sett økt aktivitet fra hacktivister mot kritisk infrastruktur i Norge og Europa, og vurderer trusselen fra hacktivisme mot spesialisthelsetjenesten som **moderat**. Med bakgrunn i den geopolitiske situasjonen vurderer vi at angrep er **mulig**.

2.2. Konsekvenser og vurdering

Det er nødvendig å forankre trusselvurderingen for spesialisthelsetjenesten i regionen og benytte den aktivt til sikkerhetsstyring. Sykehuspartner HF må vurdere i hvilken grad vi er motstandsdyktige og gjøre eventuelle tilpasninger.

Det interregionale etterretningsarbeidet som er etablert i forbindelse med utarbeidelsen av rapporten, vil i tillegg til trusselvurderingen publisere temarapporter hvor det skal gås mer i dybden på enkelte temaer. Temarapportene vil være unntatt offentlighet for å gjøre det mulig å ta med informasjon som gjør rapportene mer relevante for de som skal bruke dem. Temarapportene kan også inneholde forslag til tiltak basert på den aktuelle trusselen.

Temarapporten «Offensiv KI» ble publisert i løpet av mai 2026. De øvrige temarapportene vil bli publisert fortløpende ettersom de blir ferdigstilt.

3 Administrerende direktørs anbefaling

Det kreves en helhetlig tilnærming til sikkerhetsarbeidet, med grunnleggende og gode sikkerhetsbarrierer, for å motstå avanserte cyberangrep. Disse må kunne stoppe både opportunistiske angrepsforsøk og angrep fra avanserte aktører. Spesialisthelsetjenesten må derfor ha velutviklede metoder for å avdekke uønsket aktivitet, for å håndtere denne aktiviteten og for å igangsette nødvendige risikoreduserende tiltak.

Administrerende direktør anbefaler at styret tar *Trusselvurdering for spesialisthelsetjenesten 2026* til etterretning, og ber om at den legges til grunn for sikkerhets- og risikostyringen i foretaksgruppen.

Trykte vedlegg:

- Trusselvurdering for spesialisthelsetjenesten 2026

Utrykte vedlegg:

- Rapport på Offensiv KI (Unntatt offentlighet)